Hard pass

Des mots de passe générés sur hardware

Da Silva Bruno

Lizzi Dimitri

Sousa Claudio

Latest version http://goo.gl/P8PxBZ

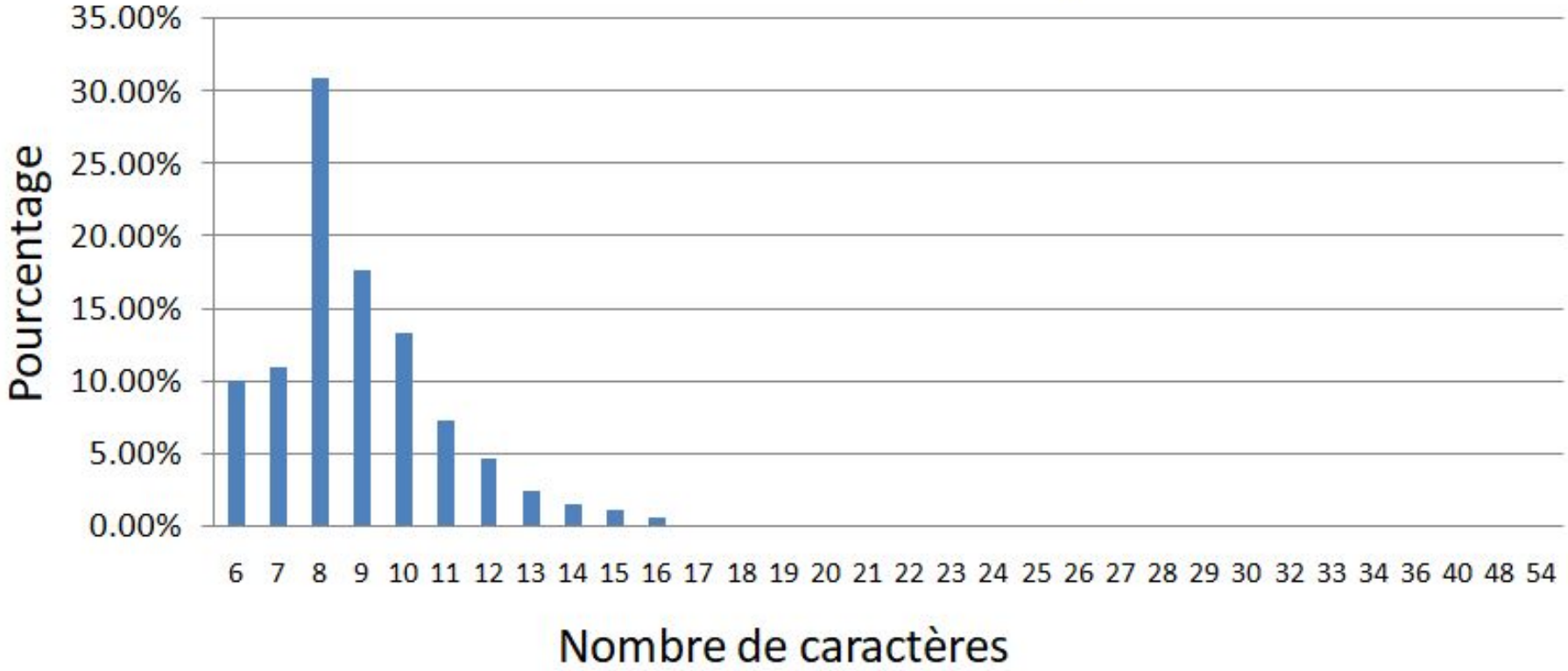
Vos mots de passe ne sont pas en sécurité !

- “In 2016, billions of accounts were leaked to internet from LinkedIn, Tumblr, MySpace, Last.FM, Yahoo!, VK.com and Gmail”
  http://thehackernews.com/2017/03/gmail-yahoo-password-hack.html
- “LastPass Leaking Passwords Via Chrome Extension”
  https://www.darknet.org.uk/2017/03/lastpass-chrome-extension-leaking-passwords/
- Demo: https://haveibeenpwned.com/

Étude : accès public aux mots de passe

Longueur des mots de passe décryptés

5'604'506 mots de passe décryptés

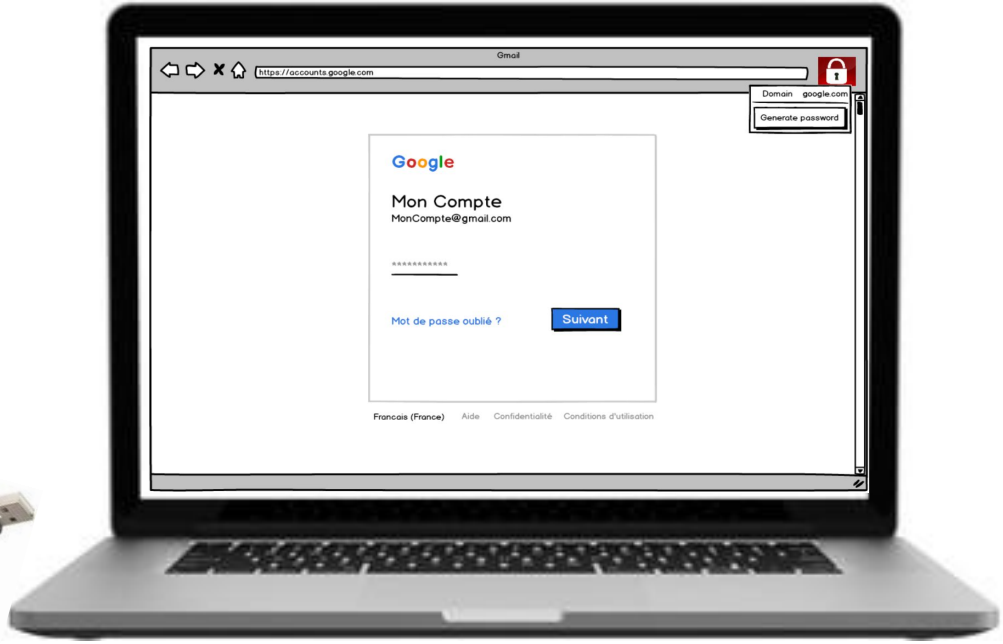


Notre solution

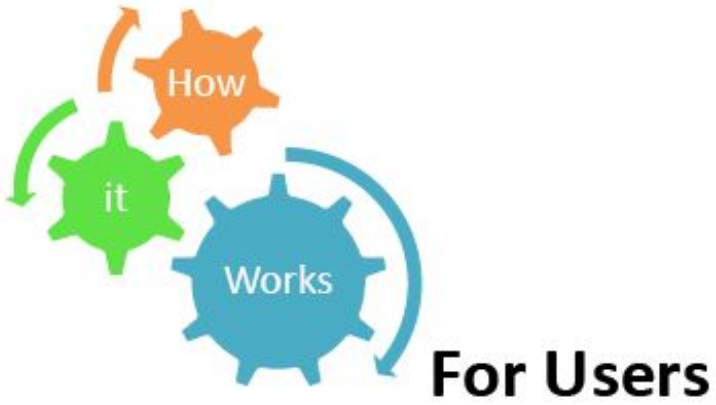
- Un seul mot de passe « maître » à mémoriser
- Mot de passe généré pour chaque domaine

```
domain_pwd = hash(master_pwd, domain, variant)
```

Notre proposition: architecture

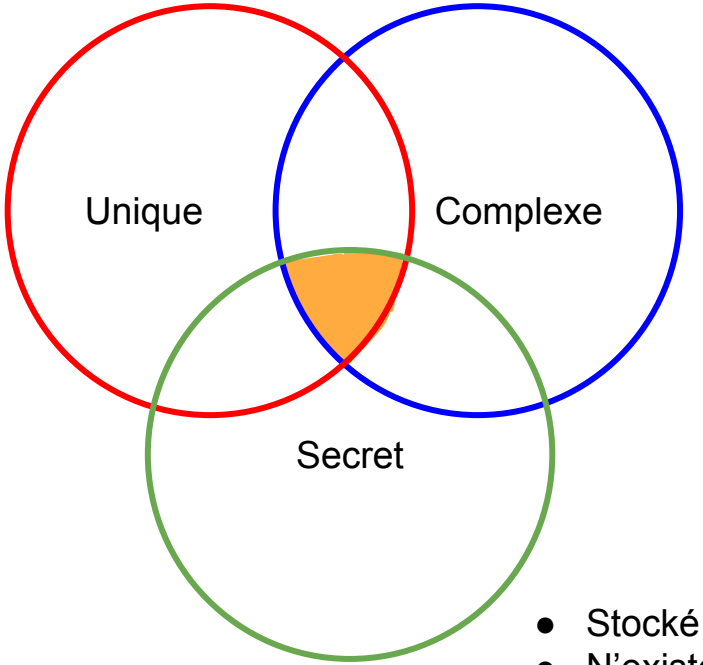


Demonstration



Respect des trois critères

- Non réutilisé
- Non prévisible



- Riche jeu de caractères
- Long

- Stocké nulle part
- N’existe que dans votre tête

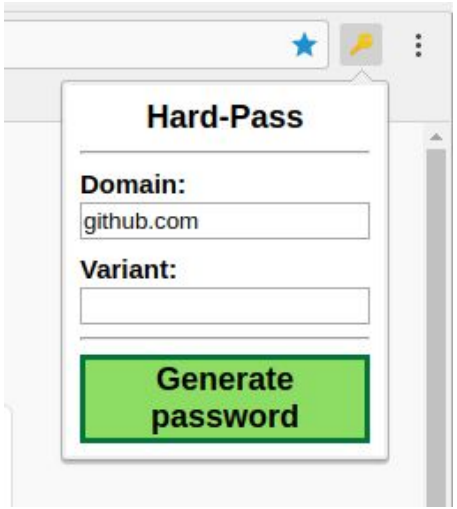
Microcontroller

- Comparatif écrans et librairies
- Clavier tactile
- Gestion des préférences utilisateur
- Hachage en SHA1
- Machine d’états
- Ajout haut-parleur
- Interface utilisateur

PlatformIO IDE for Atom

Extension

- Multi-browser
- Transformation hash -> mot de passe
- Injection du mot de passe
- Alias FQDN
- Longueur customizable
- Interface utilisateur



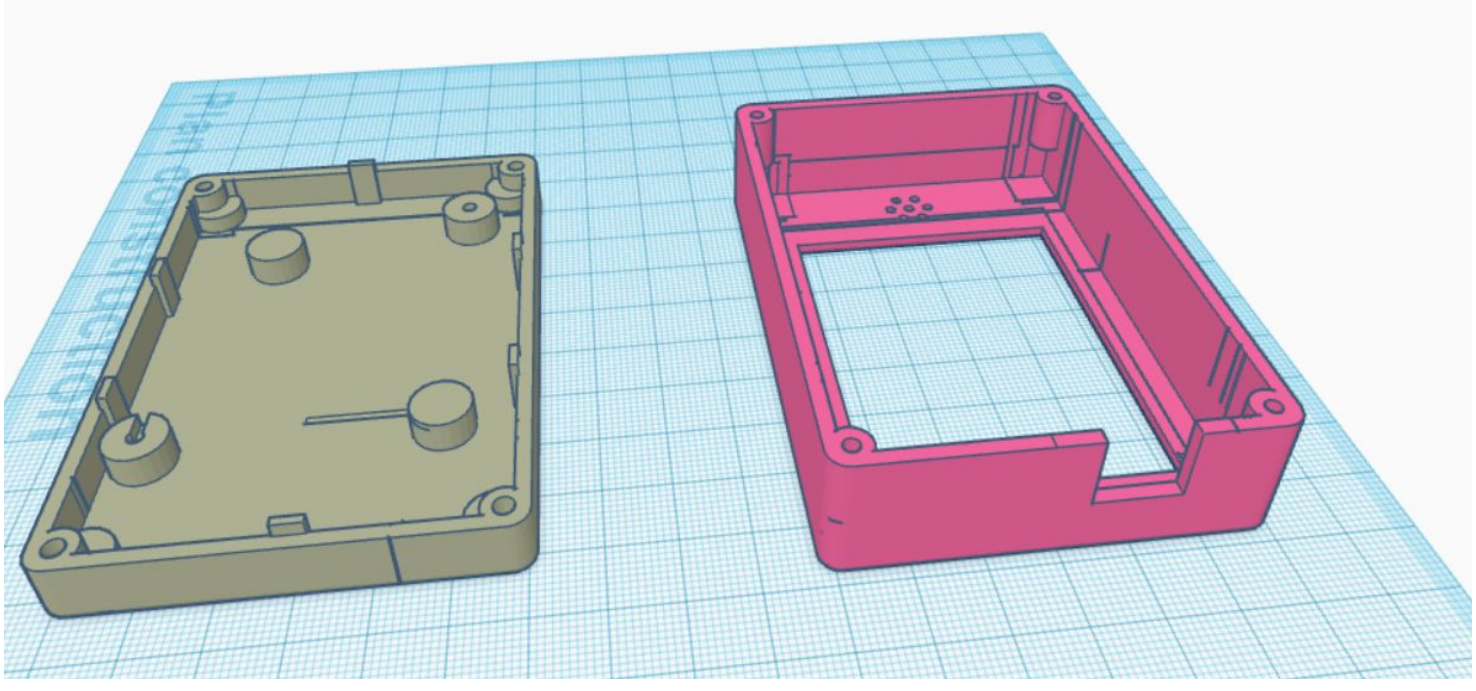
Bridge

python™

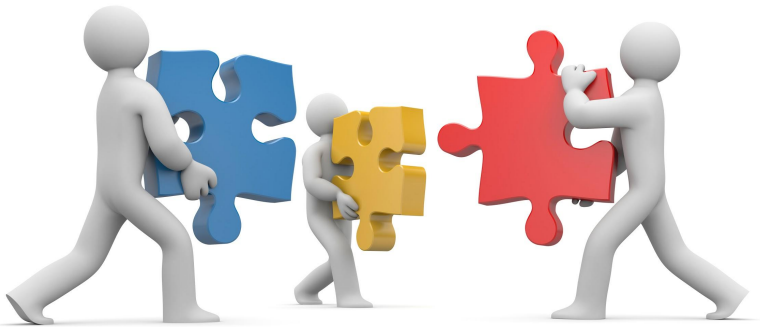
- Communication extension & micro-controller
- Multi-platform
- Packaging binaire
- Reconnection automatique

Boitier

- Modelisation 3D
- Impression



Repartition du travail



TODO hardpass

File Edit View Insert Format Data Tools Add-ons Help All changes saved in Drive

claudio.sousa@gmail.com

Comments Share

100% $ % .0 .00 123 Arial 10 More

In progress

	A	B	C	D	E
1					
2	Priority	Task	Assignee	Status	Notes
3	0	Find working touch screen	Claudio	Done	
4	0	Draw keyboard	Claudio	Done	
5	0	Create 3D model	Bruno + Claudio	Done	
6	1	Hash hardware	Claudio	Done	
7	1	Protocol estension->device	Dimitri	Done	
8	1	Extension var field	Dimitri	Done	
9	1	Bridge on reconnect reidentify right port	Dimitri	Done	
10	1	Hash: use pwd;var;domain	Claudio	Done	
11	1	Redo device screens	Bruno	Done	
12	2	Convert hash -> pwd	Dimitri	Done	
13	2	Chnage settings 'Save' in 'OK'	Bruno	Done	
14	2	domain alias in extension	Dimitri	Done	
15	2	Handle remember password on/off	Claudio	Done	
16	2	Print cases	Claudio + Bruno	In progress	
17	2	Bridge: connect only on req received	Dimitri	Done	Implemented auto-reconnection on failure instea
18	3	Truncate pwd with exceptions	Dimitri	Done	google, paypal,postfinance, ubs,etc
19	3	Test pwd injection multiple pages	Dimitri	Done	/!\ Can't find a page that doesn't work
20	3	Add keyboard shortcut to extension	Dimitri	Done	
21	3	Refactor split code page vs extension	Dimitri	Done	
22	4	Navigate to settings from home screen	Claudio	Done	
23	4	Options screen logic	Claudio	Done	
24	4	Options screen UI	Bruno	Done	
25	5	Beautify extension	Bruno	Done	
26	5	Sounds:touch + msg received	Bruno	Done	
27	3	INsert on input[type="password"]:visible	Dimitri	Done	
28	3	Domain above Variant and read-only + aufo-fill	Bruno + Claudio	Done	
29	6	Test device mem leak on multiple page switch	Claudio	Done	
30	6	Test extension on all browsers	Bruno	Done	
31	7	Color '*' button	Bruno	Done	
32	7	Bridge: packaging	Dimitri	Done	
33	7	Handle orientation in touch logic	Claudio	Done	
34	7	"Insert master pwd" placeholder in device first screen	Claudio	Done	
35	7	Solder piezzo * 2	Claudio	Done	
36	7	Redo screens title: fon size 3 and no box	Bruno	Done	
37	9	Final Presentation	ALL	In progress	
38					

Sheet1

Améliorations possibles

- Automatiser lancement du bridge
  - Hard pass device with read-only storage device + autorun
- Améliorer integration extension->page web
  - Proposer login inline
- Jumper hardware pour empêcher la mise à jour
- Mécanisme visuel d'encryption certifiée

Q & A